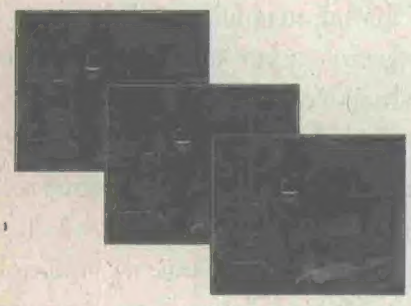
■ กองบรรณาธิการ

IT SECURITY
Computer - Network
Security and Information Protection



ความปลอดภัย ในเครือข่าย

ดูแลและป้องกันไม่ให้ตนเอง
เป็นช่องทางผ่านของแครกเกอร์
หาวิธีการป้องกันและแก้ไขจุดบกพร่อง
ของซอฟต์แวร์ที่ใช้งาน

ในโลกแห่งอุดมคติ ผู้ใช้เครือข่ายไม่ต้องกังวลว่าจะมีใครเข้ามาลักลอบใช้บัญชีโดยไม่ได้รับอนุญาต หรือผู้ดูแลระบบไม่ต้องคอยตรวจจับว่าเซิร์ฟเวอร์ที่ให้บริการมีผู้เข้ามาก่อกวนระบบหรือทำลายข้อมูล และบริษัทที่ประกอบธุรกิจไม่ต้องติดตั้งระบบป้องกันภัย เพราะจะไม่มีผู้ลักลอบเข้ามานำข้อมูลทางการค้าที่สำคัญนำไปให้กับบริษัทคู่แข่ง แต่ทว่าในโลกแห่งความเป็นจริงอย่างเช่นอินเทอร์เน็ตนั้น การบุกรุก ก่อกวน ลักลอบใช้ และทำลายระบบเป็นเรื่องที่พบเห็นได้ในชีวิตประจำวันของสังคมเครือข่าย และหลายต่อหลายครั้งที่เป็นกรณีใหญ่ที่สร้างความเสียหายเข้าขั้นอาชญากรรมทางเครือข่าย

ไม่มีใครทราบอย่างแน่ชัดว่ามีผู้ใช้อินเทอร์เน็ตทั่วโลกเป็นจำนวนเท่าใด นอกจากจะคาดประมาณไว้ว่าน่าจะมีผู้ใช้อินเทอร์เน็ตอยู่ราว 100 ล้านคน ใช้งานโฮสต์ที่ต่อเชื่อมอยู่ราว 10 ล้านเครื่องในเครือข่ายที่เชื่อมโยงกันนับแสนเครือข่าย สังคมซึ่งเป็นที่รวมของผู้คนจำนวนมากเช่นอินเทอร์เน็ตนี้ย่อมมีผู้คนส่วนหนึ่งที่เป็นนักสร้างปัญหาและก่อกวนสร้างความเสียหายให้ระบบ นับตั้งแต่มือสมัครเล่นที่ทำเพื่อความสนุกไปจนกระทั่งถึงระดับอาชญากรมืออาชีพ

ปรัชญาความปลอดภัยในอินเทอร์เน็ต

อินเทอร์เน็ตมีความปลอดภัยมากน้อยเพียงใด? คำถามนี้ดูเหมือนจะตอบโดยรวมได้ยาก เนื่องจากขอบเขตของอินเทอร์เน็ตครอบคลุมเครือข่ายจำนวนมากมาย บางเครือข่ายมีระบบรักษาความปลอดภัยอย่างเข้มงวดแม้มืออาชีพก็ยากที่จะบุกรุก บางเครือข่ายอาจไม่มีระบบป้องกันใด ๆ แครกเกอร์มือสมัครเล่นอาจเข้าไปสร้างความยุ่งยากได้ ระบบคอมพิวเตอร์ส่วนใหญ่ในอินเทอร์เน็ตที่ทำหน้าที่เป็นตัวให้บริการข้อมูลมักทำงานภายใต้ระบบปฏิบัติการยูนิกซ์ คำถามสำคัญต่อมาก็คือยูนิกซ์เป็นระบบที่มีความปลอดภัยเพียงใด

ยูนิกซ์เป็นระบบปฏิบัติการที่แรกเริ่มออกแบบขึ้นเพื่อการสื่อสารและแลกเปลี่ยนทรัพยากรข้อมูลระหว่างเครื่องโดยไม่เน้นถึงเรื่องความปลอดภัยของข้อมูล จนกระทั่งเมื่อแพร่หลายออกไปสู่ภาคธุรกิจจึงได้ปรับปรุงให้มีกลไกด้านการรักษาความปลอดภัยเพิ่มขึ้น แต่ทั้งนี้มิได้หมายความว่ายูนิกซ์เป็นระบบปฏิบัติการที่มีความปลอดภัยน้อยกว่าระบบปฏิบัติการอื่น ๆ เนื่องจากธรรมชาติของระบบปฏิบัติการแบบเปิดหรือกึ่งเปิดที่มีให้เลือกใช้อย่างแพร่หลายย่อมจะมีช่องทางให้ค้นหาจุดอ่อนด้านความปลอดภัยได้ง่าย

หากจะขีดวงจำกัดอยู่เฉพาะในระบบปฏิบัติการยูนิกซ์เพียงอย่างเดียวและแยกพิจารณาถึงยูนิกซ์เชิงการค้าเช่น โซลาริส เอไอเอ็กซ์ เอชพี-ยูเอ็กซ์ ไอริกซ์ หรืออัลทริกซ์ กับยูนิกซ์ที่เป็นสาธารณะ เช่น ลีนุกซ์ หรือฟรีบีเอสดี ก็ไม่สามารถสรุปได้ว่ายูนิกซ์เชิงการค้ามีความปลอดภัยสูงกว่ายูนิกซ์ที่เป็นสาธารณะ แต่เนื่องจากรูปแบบที่มีให้บริการอย่างหลากหลายเมื่อมองโดยภาพรวมแล้วจึงกล่าวได้ว่าความปลอดภัยในยูนิกซ์มีจุดอ่อนให้โจมตีได้มาก การระมัดระวังรักษาความปลอดภัยในระบบเครือข่ายจึงไม่ใช่เพียงแต่พึ่งพาขีดความสามารถของระบบปฏิบัติการเท่านั้น แต่ยังต้องการ นโยบายรักษาความปลอดภัย (Security Policy) ซึ่งเป็นตัวกำหนดขอบเขตการใช้งานและมาตรการดำเนินการรักษาความปลอดภัยโดยรวมทั้งระบบ

รูปแบบการโจมตีทางเครือข่าย

นอกเหนือไปจากการหาช่องโหว่หรือข้อบกพร่องของซอฟต์แวร์ที่ให้บริการในเซิร์ฟเวอร์และเจาะเข้าสู่ระบบโดยได้สิทธิผู้ใช้ระดับสูงสุดแล้ว แครกเกอร์มักใช้วิธีโจมตีเพื่อสร้างปัญหากับระบบในรูปแบบต่าง ๆ ที่จัดออกได้เป็นกลุ่มดังนี้

ทำลายระบบ (destructive method)

วิธีนี้คือการใช้ซอฟต์แวร์เข้ามาก่อกวนหรือสร้างภาระงานหนักให้ระบบ เช่น ใช้โปรแกรมสร้างภาระให้เราเตอร์หรือเมล์เซิร์ฟเวอร์หยุดการทำงานจนกระทั่งผู้ใช้ไม่สามารถเข้าใช้บริการได้ วิธีนี้ถึงแม้ไม่ได้บุกรุกเข้ามาเพื่อให้ได้สิทธิ์การใช้ระบบ แต่ก็สร้างปัญหาให้ระบบไม่สามารถดำเนินการต่อไปได้ กรรมวิธีที่นิยมใช้โดยทั่วไปคือ

- การส่งอีเมล์ขนาดใหญ่จำนวนมาก หรือ เมล์บอมบ์ (mail bomb) ผู้เปิดอ่านจดหมายจะเสียเวลาอย่างมากเมื่อต้องอ่านจดหมายซึ่งอาจมีจำนวนมหาศาลและมีขนาดใหญ่ เซิร์ฟเวอร์ที่ถูกโจมตีด้วยเมล์บอมบ์ปริมาณมากมักหยุดการทำงานลงในชั่วระยะเวลาสั้น ๆ เนื่องจากต้องใช้ทรัพยากรระบบในการรับจดหมายที่เข้ามา วิธีการป้องกันการโจมตีด้วยเมล์บอมบ์มีหลายวิธี เช่น ติดตั้งเมล์ที่จำกัดขนาดที่จะรับ การติดตั้งตัวกรองเมล์ และการตรวจจับและกำจัดเมล์ที่ได้รับ เป็นต้น

- การโจมตีจุดบกพร่องแบบ ดอส (DoS : Denial-of -Service) แครกเกอร์ใช้วิธีเข้าไปขอใช้บริการที่เครือข่ายมีให้ โดยการขอจองทรัพยากรที่มีในระบบแบบสะสมด้วยอัตราที่รวดเร็วจนกระทั่งระบบไม่มีทรัพยากรเหลือเพื่อให้บริการผู้ใช้รายอื่น วิธีการที่นิยมใช้คือการสร้างแพ็กเกตขอเชื่อมต่อโปรโตคอลทีซีพีจำนวนมาก (เรียกว่า TCP SYN Flooding) หรือการสร้างแพ็กเกตขนาดใหญ่ส่งไปยังบริการไอซีเอ็มพีด้วยคำสั่ง ping (เรียกว่า ping of death) การแก้ปัญหาการโจมตีแบบนี้จะต้องติดตั้งซอฟต์แวร์ทีซีพีซึ่งไม่กินทรัพยากรระบบไว้นานเกินไป นอกจากนี้ยังมีการโจมตีในลักษณะอื่นที่เป็นที่รู้จักในหมู่แครกเกอร์ เช่น Teardrop, LAND, หรือ Winnuke เป็นต้น

การโจมตีแบบบรูทฟอร์ซ (brute-force attack)

ผู้บุกรุกจะใช้โปรแกรมเชื่อมต่อด้วยเทลเน็ตไปยังเซิร์ฟเวอร์ปลายทาง โปรแกรมจะคาดเดาชื่อบัญชีจากชื่อมาตรฐานทั่วไปที่มีอยู่และสร้างรหัสผ่านขึ้นมาเพื่อเข้าใช้บัญชีนั้นโดยอัตโนมัติ โปรแกรมจะมีดิคชันนารีเพื่อเป็นฐานสำหรับใช้สร้างรหัสผ่านโดยคำนวณหารูปแบบรหัสผ่านที่เป็นไปได้ เช่น รหัสผ่านที่ตรงกับชื่อบัญชีหรือรหัสที่เขียนย้อนกลับ หรือรหัสผ่านที่เป็นคำที่พบได้ในดิคชันนารี หรือคำประสม เป็นต้น การโจมตีแบบนี้มักนิยมใช้ในหมู่แครกเกอร์มือใหม่เนื่องจากมีเครื่องมือที่หาได้ง่ายและใช้งานสะดวก แต่ก็เป็นวิธีที่ตรวจสอบและค้นหาต้นตอได้ง่ายเช่นกัน เนื่องจากเซิร์ฟเวอร์ปลายทางจะมีระบบบันทึกการเข้าใช้งานทั้งที่สำเร็จและไม่สำเร็จ

การโจมตีแบบพาสซีฟ (passive attack)

แครกเกอร์อาจไม่จำเป็นต้องใช้วิธีเจาะเข้าไปยังเครื่องปลายทางโดยตรง หากแต่ติดตั้งโปรแกรมตรวจจับแพ็กเกต (packet sniffing) ไว้ในที่ใดที่หนึ่ง (หรือที่รู้จักกันดีในชื่อของสนิฟเฟอร์) เมื่อมีการเชื่อมขอใช้บริการไปยังเซิร์ฟเวอร์อื่น ชื่อบัญชีและรหัสผ่านที่ป้อนผ่านแป้นพิมพ์จะถูกบันทึกเก็บไว้และรายงานไปยังแครกเกอร์ เนื่องจากข้อมูลที่วิ่งอยู่ในเครือข่ายนั้นมักเป็นข้อมูลดิบที่ไม่มีการเข้ารหัสลับ แครกเกอร์สามารถจะดักจับรหัสผ่านของทุกคนที่เข้าใช้งานระบบได้ไม่เว้นแม้แต่ผู้ดูแลระบบเอง ไม่ว่าผู้ใช้ใดจะเปลี่ยนรหัสผ่านไปกี่ครั้งก็ตาม แครกเกอร์ก็จะได้รหัสใหม่นั้นทุกครั้ง เทคนิคของการใช้สนิฟเฟอร์จำเป็นต้องใช้ความรู้ขั้นก้าวหน้าขึ้นมาอีกระดับหนึ่ง โดยปกติแล้วการตรวจหาว่าเซิร์ฟเวอร์มีสนิฟเฟอร์ซ่อนอยู่หรือไม่อาจทำได้โดยไม่ยากนัก แต่แครกเกอร์ที่เชี่ยวชาญมักวางหมากขั้นที่สองโดยการเปลี่ยนแปลงโปรแกรมตรวจสอบ

เพื่อไม่ให้รายงานผลว่ามีสนิฟเฟอร์ซ่อนอยู่ วิธีการป้องกันสนิฟเฟอร์อีกรูปแบบหนึ่งก็คือการใช้เซลล์ที่ผ่านการเข้ารหัสลับทำให้ไม่สามารถนำดูข้อมูลดิบได้

กล่องเครื่องมือแครกเกอร์

เทคนิคการเจาะเข้าสู่ระบบยูนิกซ์มีตั้งแต่วิธีพื้น ๆ ที่ไม่ได้ใช้เทคนิคหรือเครื่องใด เรื่อยไปจนกระทั่งเทคนิคที่ซับซ้อน แต่เป็นที่น่าสังเกตว่าพวกแครกเกอร์เพียงแต่ใช้วิธีพื้นฐานง่าย ๆ ก็สามารถเจาะเข้าสู่ระบบได้

เดาสุ่มทุกทาง

ด่านสำคัญในการเข้าสู่ยูนิกซ์คือรหัสผ่านซึ่งเก็บอยู่ในแฟ้ม /etc/passwd รหัสผ่านในแฟ้มนี้จะผ่านการเข้ารหัสลับทำให้ไม่ทราบถึงรหัสต้นฉบับได้ แต่แฟ้ม /etc/passwd ไม่ได้เป็นแฟ้มลับ ในทางตรงข้ามกลับเปิดโอกาสให้ผู้ใช้ทุกคนเปิดอ่านได้ แครกเกอร์ซึ่งได้แฟ้มรหัสผ่านจะนำแฟ้มไปผ่านโปรแกรมวิเคราะห์ทารหัส โดยตัวโปรแกรมจะสร้างรหัสต้นฉบับขึ้นมาจากดิคชันนารีที่มีอยู่ในระบบ (เช่นในยูนิกซ์คือ /usr/dict) แล้วเข้ารหัสเพื่อนำผลที่ได้ไปเปรียบเทียบกับรหัสใน /etc/passwd

โปรแกรมแกะรหัสผ่านเป็นโปรแกรมเขียนได้ง่าย ต้นฉบับโปรแกรมภาษาซีอาจมีความยาวเพียง 60–70 บรรทัด อีกทั้งยังมีโปรแกรมสำเร็จที่เผยแพร่ในอินเทอร์เน็ตอยู่แล้วเช่น crack (ftp://ftp.cert.org/pub/tools/crack)

crack สร้างขึ้นเพื่อจุดประสงค์ให้ผู้ดูแลระบบใช้วิเคราะห์หาว่าผู้ใช้รายใดตั้งรหัสผ่านง่ายเกินไป แต่ก็มีผู้นำไปใช้ผิดวัตถุประสงค์ หนทางที่ป้องกันได้ส่วนหนึ่งก็คือผู้ใช้ทุกคนจะต้องเรียนรู้หลักการและตั้งรหัสผ่านที่คาดเดาได้ยาก

ยูนิกซ์ในระบบ SystemV จะใช้วิธีแยกเอาส่วนของรหัสผ่านไปเก็บไว้ในแฟ้มต่างหากอีกแฟ้มหนึ่งที่ไม่อนุญาตให้ผู้ใช้ทั่วไปอ่านได้ กรรมวิธีแบบนี้เรียกว่าระบบ "shadow password"

สนิฟเฟอร์

สนิฟเฟอร์เป็นชื่อเครื่องหมายทางการค้าของระบบตรวจจับแพ็กเกตเพื่อนำมาวิเคราะห์และตรวจหาปัญหาในเครือข่าย ตัวระบบจะประกอบด้วยคอมพิวเตอร์ที่มีการ์ดเครือข่ายสมรรถนะสูงและซอฟต์แวร์ตรวจวิเคราะห์แพ็กเกต แต่ในปัจจุบันมีซอฟต์แวร์จำนวนมากที่มีขีดความสามารถระดับเดียวกับสนิฟเฟอร์ และทำงานได้โดยไม่ต้องพึ่งฮาร์ดแวร์เฉพาะ อีกทั้งมีแพร่หลายในแทบทุกระบบปฏิบัติการ ชื่อสนิฟเฟอร์ในปัจจุบันจึงนิยมใช้เป็นชื่อเรียกของโปรแกรมใด ๆ ที่สามารถตรวจจับและวิเคราะห์แพ็กเกตไปโดยปริยาย

จารชนอินเทอร์เน็ต

ผู้ใช้อินเทอร์เน็ตแรกเริ่มนั้นจำกัดอยู่เพียงกลุ่มนักวิชาการ ตราบกระทั่งเครือข่ายขยายออกไปทั่วโลก เปิดโอกาสให้บุคคลทุกระดับทุกอาชีพมีสิทธิ์เป็นสมาชิกคนหนึ่งในสังคมอินเทอร์เน็ตได้ ความปลอดภัยของข้อมูลเริ่มเป็นสิ่งที่ต้องระมัดระวังมากยิ่งขึ้น ในระยะเวลาที่ผ่านมามีการลักลอบเข้าไปใช้เครื่องในศูนย์คอมพิวเตอร์ใหญ่ ๆ หลายต่อหลายครั้ง ถึงแม้ว่าบางครั้งจะจับได้แต่ก็ต้องอาศัยความพยายามและเทคนิคในการสะกดรอยด้วยความยากลำบากกว่าจะทราบได้ว่าจารชนเหล่านี้แฝงกายอยู่ที่มุมใดในโลก

เรามักจะเรียกพวกที่มีความสามารถเจาะเข้าสู่ระบบคอมพิวเตอร์ว่า "แฮกเกอร์" (Hacker) ซึ่งความหมายดั้งเดิมที่แท้จริงแล้ว แฮกเกอร์สื่อความหมายถึงผู้เชี่ยวชาญด้านโอเอสหรือระบบ สามารถเข้าไปแก้ไข ดัดแปลงการทำงานระดับลึกได้ หรือในสารบบของความปลอดภัยแล้ว แฮกเกอร์เป็นอาชีพหนึ่งที่ทำหน้าที่เจาะระบบและค้นหาจุดอ่อนเพื่อหาหนทางแก้ไขป้องกัน ส่วนพวกที่เจาะระบบเข้าไปโดยไม่ประสงค์ดีมีชื่อเรียกโดยเฉพาะว่า "แครกเกอร์" (Cracker) พวกหลังนี้เข้าข่ายจารชนอิเล็กทรอนิกส์ที่มักชอบก่อกวนสร้างความวุ่นวายหรือทำงานเป็นมืออาชีพที่คอยล้วงความลับหรือข้อมูลไปขาย แต่จะทำอย่างไรได้เมื่อคำว่าแฮกเกอร์ใช้ผิดความหมายจนติดปากไปโดยปริยายเสียแล้ว

ม้าโทรจัน

โปรแกรมม้าโทรจันเป็นโปรแกรมที่ลวงให้ผู้ใช้งานเข้าใจผิดว่าเป็นโปรแกรมปกติโปรแกรมหนึ่งที่ใช้งานอยู่เป็นประจำ แต่การทำงานจริงกลับเป็นการดักจับข้อมูลเพื่อส่งไปให้แครกเกอร์ ตัวอย่างเช่นโปรแกรมโทรจันที่ลวงว่าเป็นโปรแกรมล็อกอินเข้าสู่ระบบ เมื่อผู้ใช้ป้อนบัญชีและรหัสผ่านก็จะแอบส่งรหัสผ่านไปให้แครกเกอร์

ประตูกล

แครกเกอร์ใช้ ประตูลับ (backdoors) ซึ่งเป็นวิธีพิเศษเข้าสู่ระบบโดยไม่ได้รับอนุญาต ความหมายของประตูลับอาจรวมไปถึงวิธีการที่ผู้พัฒนาโปรแกรมทิ้งรหัสพิเศษหรือเปิดทางเฉพาะไว้ในโปรแกรมโดยไม่ให้ผู้ใช้ล่วงรู้ แครกเกอร์ส่วนใหญ่จะมีชุดซอฟต์แวร์ซึ่งสร้างขึ้นเพื่อเจาะเข้าสู่ระบบตามจุดอ่อนที่มีอยู่ด้วยวิธีการต่าง ๆ

ซอฟต์แวร์ตรวจช่องโหว่ระบบ

ในอินเทอร์เน็ตมีซอฟต์แวร์เป็นจำนวนมากที่ใช้ในการตรวจวิเคราะห์หารูโหว่ของระบบรักษาความปลอดภัย ซอฟต์แวร์เหล่านี้เผยแพร่โดยไม่คิดมูลค่าและเป็นเสมือนดาบสองคมที่ทั้งแฮกเกอร์และแครกเกอร์นำไปใช้ด้วยจุดประสงค์ที่ต่างกัน ซอฟต์แวร์ในกลุ่มนี้ซึ่งเป็นที่รู้จักแพร่หลายได้แก่ Internet Security Scanner, SATAN, COPS และ Tiger เป็นต้น

การป้องกันและระวังภัย

ในปัจจุบันมีซอฟต์แวร์และฮาร์ดแวร์หลากหลายที่ใช้เป็นเครื่องมือรักษาความปลอดภัยในระบบ ตัวอย่างของซอฟต์แวร์รักษาความปลอดภัยเบื้องต้นได้กล่าวไปในหัวข้อที่แล้ว ส่วนซอฟต์แวร์ที่ติดตั้งเป็นระบบรักษาความปลอดภัยที่กำลังเริ่มใช้อย่างแพร่หลายได้แก่ระบบไฟร์วอลล์ (Firewall) ซึ่งเป็นซอฟต์แวร์ทำหน้าที่เสมือนกับกำแพงกันไฟไม่ให้ลุกลามขยายตัวหากมีไฟไหม้เกิดขึ้น

ไฟร์วอลล์จะอาศัยคอมพิวเตอร์เครื่องหนึ่งเป็นด่านเข้าออกเครือข่ายและเป็นเสมือนกำแพงกันไฟ และมีซอฟต์แวร์ที่ผู้ดูแลระบบจะติดตั้งและกำหนดรูปแบบการอนุญาตให้เข้าใช้เครือข่าย

อินเทอร์เน็ตมีหน่วยงาน CERT (Computer Emergency Response Team) ทำหน้าที่เป็นเสมือน "ตำรวจอินเทอร์เน็ต" คอยดูแลความปลอดภัยในเครือข่ายอินเทอร์เน็ตทั่วโลก อย่างไรก็ตาม หน่วยงาน CERT ไม่ได้มีอำนาจในการจัดการหรือจับกุมแครกเกอร์ หากเพียงแต่คอยทำหน้าที่เตือนและช่วยเหลือตลอดจนแจ้งข่าวเมื่อพบปัญหาด้านความปลอดภัยในระบบเพื่อให้ผู้ดูแลระบบสามารถแก้ไขได้ทันท่วงที CERT จะประกาศข่าวเตือนภายใต้หัวข้อข่าว comp.security.announce เป็นประจำ

ส่งท้าย

ไม่ว่าระบบเครือข่ายจะมีฮาร์ดแวร์หรือซอฟต์แวร์ที่ดีเพียงใดในการปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่งก็คือผู้ใช้งานในระบบจะต้องคอยช่วยสอดส่องดูแล และป้องกันไม่ให้ตนเองเป็นช่องทางผ่านของแครกเกอร์ ผู้ดูแลระบบจะต้องคอยติดตามและหาวิธีการป้องกันและแก้ไขจุดบกพร่องของซอฟต์แวร์ที่ใช้งาน พึงระลึกไว้ว่าไม่มีระบบเครือข่ายใดที่ปลอดภัยร้อยเปอร์เซ็นต์จากแครกเกอร์